(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－56473

(43)公開日　平成10年(1998)２月24日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ　12/46			Ｈ０４Ｌ　11/00	３１０Ｃ	
12/28					

審査請求　未請求　請求項の数32　ＯＬ　（全 13 頁）

(21)出願番号　特願平9－149743

(22)出願日　平成９年(1997)６月６日

(31)優先権主張番号　特願平8－145854

(32)優先日　平８(1996)６月７日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　谷本　茂明
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　中島　彦之
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　磯田　邦彦
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(74)代理人　弁理士　志賀　正武

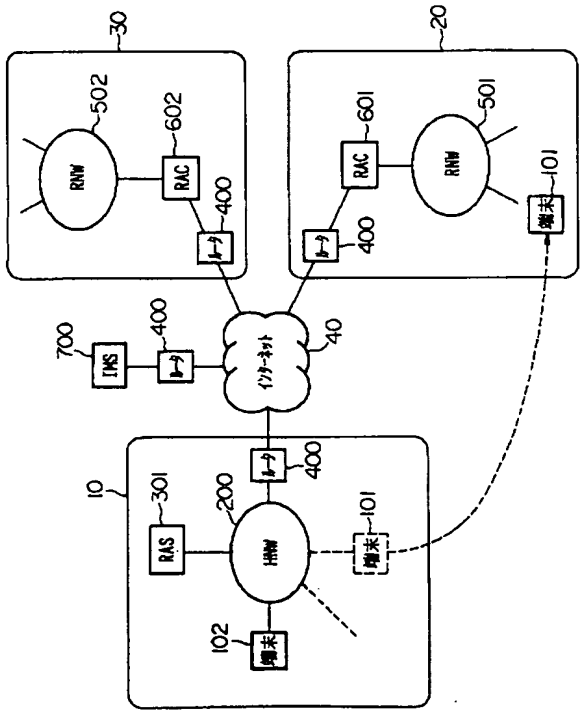
最終頁に続く

(54)【発明の名称】　仮想ＬＡＮ制御システム及び方法ならびに仮想ＬＡＮ管理サーバ

(57)【要約】

【課題】　端末離脱の検出を端末に特別なシステムや手順を設定することなく実現する。

【解決手段】　端末１０１がホームネットワーク２００からリモートネットワーク５０１に移動して管理されている時、該端末が送出するパケットのタイミングまたは該端末が更に他のリモートネットワーク５０２に移動した場合の接続情報に基づき、端末とホームネットワークとのアクセスを制御するリモートアクセスサーバ３０１、リモートネットワークとインターネット４０との通信を制御するリモートアクセスクライアント、端末の接続位置及びパケット送信を管理する仮想ＬＡＮ管理サーバ７００を用いて端末１０１の当該リモートネットワークからの離脱を検出し、端末離脱に伴うシステムの管理内容変更の制御を行う。



1

【特許請求の範囲】

【請求項１】　１つ以上の端末が通常時接続されるホームネットワークと、前記端末が移動時に接続される少なくとも１つのリモートネットワークとがグローバル・ネットワークを介して接続された仮想的なＬＡＮにおいて、

前記ホームネットワークに接続され、前記グローバル・ネットワークのアドレスを有し、接続中の各端末の接続位置を示す管理テーブルを具備して、端末が前記リモートネットワークの１つに移動した時に、該端末と前記ホームネットワークとのアクセスを、該端末が前記ホームネットワーク内でアクセスしているかのように制御するリモートアクセスサーバと、

前記各リモートネットワークに接続され、前記グローバル・ネットワークのアドレスを有し、該リモートネットワークに接続中の各端末と前記ホームネットワークとの対応関係を示す管理テーブルを具備して、前記リモートネットワークと前記グローバル・ネットワークとの通信を制御するリモートアクセスクライアントと、

前記グローバル・ネットワークに接続され、該グローバル・ネットワークのアドレスを有し、各端末と前記リモートアクセスサーバの対応関係及び、接続中の各端末の接続位置を示す管理テーブルを具備して、端末の接続位置及びパケット送信を管理する仮想ＬＡＮ管理サーバとを有し、

いずれかの端末が前記リモートネットワークの１つに接続され管理されている場合、該端末が送出するパケットのタイミングまたは該端末が更に他のリモートネットワークに移動した場合の接続情報に基づいて当該端末の当該リモートネットワークからの離脱を検出し、前記仮想ＬＡＮ管理サーバを介して端末離脱に伴うシステムの管理内容変更の制御を行うことを特徴とする仮想ＬＡＮ制御システム。

【請求項２】　前記端末離脱の検出において、

各リモートアクセスクライアントは、接続中の前記端末がパケットを送出する毎に、自動的にタイマ値が増加する監視タイマをその端末用にセットし、該タイマ値が所定のスレッシュホールド値を超えた時に当該端末が離脱したと判定し、前記仮想ＬＡＮ管理サーバに端末の離脱を通知することを特徴とする請求項１記載の端末離脱検出システム。

【請求項３】　前記リモートネットワークとして２つ以上のリモートネットワークが設けられており、

前記端末離脱の検出において、端末が接続管理下の第１のリモートネットワークから第２のリモートネットワークに移動した場合、

該端末がパケットを送出すると、前記第２のリモートネットワークのリモートアクセスクライアントはこれを検出して端末が接続されたことを前記仮想ＬＡＮ管理サーバに通知し、

2

通知を受けた前記仮想ＬＡＮ管理サーバは、自身の管理テーブルを検索し、該端末がそれまで接続していたリモートネットワークが前記第１のリモートネットワークであることを認識し、該第１のリモートネットワークのリモートアクセスクライアントに該端末の離脱を通知することを特徴とする請求項１記載の端末離脱検出システム。

【請求項４】　前記端末離脱の検出において、

前記リモートアクセスクライアントが自身の管理テーブルに記録された接続中の各端末に対して所定時間毎に監視メッセージを送信し、ある当該端末から応答メッセージが返送されない場合に当該端末が離脱したと判定し、前記仮想ＬＡＮ管理サーバに端末の離脱を通知することを特徴とする請求項１記載の端末離脱検出システム。

【請求項５】　前記監視メッセージはＯＳＩのレイヤ３アドレスを含み、前記応答メッセージはＯＳＩのレイヤ２アドレスを含むことを特徴とする請求項４記載の端末離脱検出システム。

【請求項６】　前記端末離脱が検出されると、端末が離脱したリモートネットワークのリモートアクセスクライアントは、自身の管理テーブルの当該端末に関する情報を削除することを特徴とする請求項１記載の端末離脱検出システム。

【請求項７】　前記端末離脱が検出されると、

前記仮想ＬＡＮ管理サーバは、自身の管理テーブルの内容を更新するとともに、前記リモートアクセスサーバに端末の離脱を通知し、

通知を受けた前記リモートアクセスサーバは、自身の管理テーブルの内容を更新することを特徴とする請求項１記載の端末離脱検出システム。

【請求項８】　前記グローバル・ネットワークはインターネットであることを特徴とする請求項１～７いずれか記載の端末離脱検出システム。

【請求項９】　前記グローバル・ネットワークはイントラネットであることを特徴とする請求項１～７いずれか記載の端末離脱検出システム。

【請求項１０】　１つ以上の端末が通常時接続されるホームネットワークと、前記端末が移動時に接続される少なくとも１つのリモートネットワークとがグローバル・ネットワークを介して接続された仮想的なＬＡＮシステムにおける端末離脱検出方法であって、

いずれかの端末が前記リモートネットワークの１つに接続され管理されている場合、該端末が送出するパケットのタイミングまたは該端末が更に他のリモートネットワークに移動した場合の接続情報に基づいて当該端末の当該リモートネットワークからの離脱を検出し、端末離脱に伴うシステムの管理内容変更の制御を行うことを特徴とする端末離脱検出方法。

【請求項１１】　前記端末離脱の検出において、接続中の各端末がパケットを送出する毎に、自動的にタイマ値

が増加する監視タイマをその端末用にセットし、該タイマ値が所定のスレッシュホールド値を超えた時に当該端末が離脱したと判定する請求項１０記載の端末離脱検出方法。

【請求項１２】　前記リモートネットワークとして２つ以上のリモートネットワークが設けられており、
前記端末離脱の検出において、端末が接続管理下の第１のリモートネットワークから第２のリモートネットワークに移動した場合に、
当該端末のパケットの送出を検出し、
当該端末の管理情報から該端末がそれまで接続していたリモートネットワークが前記第１のリモートネットワークであることを認識し、該第１のリモートネットワークのリモートアクセスクライアントに該端末の離脱を通知する請求項１０記載の端末離脱検出方法。

【請求項１３】　前記端末離脱の検出において、
当該リモートネットワークに接続中の各端末に対して所定時間毎に監視メッセージを送信し、当該端末から応答メッセージが返送されない場合に当該端末が離脱したと判定することを特徴とする請求項１０記載の端末離脱検出方法。

【請求項１４】　前記監視メッセージはＯＳＩのレイヤ３アドレスを含み、前記応答メッセージはＯＳＩのレイヤ２アドレスを含むことを特徴とする請求項１３記載の端末離脱検出方法。

【請求項１５】　前記グローバル・ネットワークはインターネットであることを特徴とする請求項１０～１３いずれか記載の端末離脱検出方法。

【請求項１６】　前記グローバル・ネットワークはイントラネットであることを特徴とする請求項１０～１３いずれか記載の端末離脱検出方法。

【請求項１７】　１つ以上の端末が通常時接続されるホームネットワークと、前記端末が移動時に接続される少なくとも１つのリモートネットワークとがグローバル・ネットワークを介して接続された仮想的なＬＡＮシステムで用いられる仮想ＬＡＮ管理サーバであって、前記グローバル・ネットワークに接続され、該グローバル・ネットワークのアドレスを有し、各端末と前記リモートネットワークのリモートアクセスサーバの対応関係及び、接続中の各端末の接続位置を示す管理テーブルを具備して、端末の接続状態及びパケット送信を管理するものであり、
いずれかの端末が前記リモートネットワークの１つに接続され管理されている場合、該端末が更に他のリモートネットワークに移動した場合の接続情報に基づいて当該端末の当該リモートネットワークからの離脱を検出し、端末離脱に伴うシステムの管理内容変更の制御を行うことを特徴とする仮想ＬＡＮ管理サーバ。

【請求項１８】　前記仮想的なＬＡＮシステムには、前記リモートネットワークとして２つ以上のリモートネットワークが設けられており、

前記端末離脱の検出において、端末が接続管理下の第１のリモートネットワークから第２のリモートネットワークに移動し、前記第２のリモートネットワークを介して本管理サーバに端末の接続が通知された場合、
前記管理テーブルを検索し、該端末がそれまで接続していたリモートネットワークが前記第１のリモートネットワークであることを認識して該第１のリモートネットワークのリモートアクセスクライアントに該端末の離脱を通知することを特徴とする請求項１７記載の仮想ＬＡＮ管理サーバ。

【請求項１９】　前記端末離脱が検出されると前記管理テーブルの内容を更新することを特徴とする請求項１７記載の仮想ＬＡＮ管理サーバ。

【請求項２０】　１つ以上の端末が通常時接続されるホームネットワークと、前記端末が移動時に接続される少なくとも１つのリモートネットワークとがグローバル・ネットワークを介して接続された仮想的なＬＡＮシステムで用いられる仮想ＬＡＮ管理方法であって、
いずれかの端末が前記リモートネットワークの１つに接続され管理されている場合、該端末が更に他のリモートネットワークに移動した場合の接続情報に基づいて当該端末の当該リモートネットワークからの離脱を検出し、端末離脱に伴うシステムの管理内容変更の制御を行うことを特徴とする仮想ＬＡＮ管理方法。

【請求項２１】　前記仮想的なＬＡＮシステムには、前記リモートネットワークとして２つ以上のリモートネットワークが設けられており、
前記端末離脱の検出において、端末が接続管理下の第１のリモートネットワークから第２のリモートネットワークに移動し、前記第２のリモートネットワークを介して端末の接続が通知された場合、該端末の管理情報から該端末がそれまで接続していたリモートネットワークが前記第１のリモートネットワークであることを認識して該第１のリモートネットワークのクライアントに該端末の離脱を通知することを特徴とする請求項２０記載の仮想ＬＡＮ管理方法。

【請求項２２】　コンピュータに請求項２０または２１記載の方法を実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項２３】　１つ以上の端末が通常時接続されるホームネットワークと、前記端末が移動時に接続される少なくとも１つのリモートネットワークとがグローバル・ネットワークを介して接続された仮想的なＬＡＮシステムで用いられるリモートアクセスクライアントであって、前記各リモートネットワークに接続され、前記グローバル・ネットワークのアドレスを有し、該リモートネットワークに接続中の各端末と前記ホームネットワークとの対応関係を示す管理テーブルを具備して、前記リモートネットワークと前記グローバル・ネットワークとの

通信を制御し、
いずれかの端末が前記リモートネットワークの１つに接続され管理されている場合、該端末が送出するパケットのタイミング情報に基づいて当該端末の当該リモートネットワークからの離脱を検出することを特徴とするリモートアクセスクライアント。

【請求項２４】　前記端末離脱の検出において、
接続中の各端末がパケットを送出する毎に、自動的にタイマ値が増加する監視タイマをその端末用にセットし、該タイマ値が所定のスレッシュホールド値を超えた時、当該端末が離脱したと判定することを特徴とする請求項２３記載のリモートアクセスクライアント。

【請求項２５】　前記端末離脱の検出において、
前記管理テーブルに記録された接続中の各端末に対して所定時間毎に監視メッセージを送信し、該当端末から応答メッセージが返送されない場合に当該端末が離脱したと判定することを特徴とする請求項２３記載のリモートアクセスクライアント。

【請求項２６】　前記監視メッセージはＯＳＩのレイヤ３アドレスを含み、前記応答メッセージはＯＳＩのレイヤ２アドレスを含むことを特徴とする請求項２５記載のリモートアクセスクライアント。

【請求項２７】　前記端末離脱が検出されると、前記管理テーブルの当該端末に関する情報を削除することを特徴とする請求項２３記載のリモートアクセスクライアント。

【請求項２８】　１つ以上の端末が通常時接続されるホームネットワークと、前記端末が移動時に接続される少なくとも１つのリモートネットワークとがグローバル・ネットワークを介して接続された仮想的なＬＡＮシステムで用いられるリモートアクセス方法であって、
いずれかの端末が前記リモートネットワークの１つに接続され管理されている場合、該端末が送出するパケットのタイミング情報に基づいて当該端末の当該リモートネットワークからの離脱を検出することを特徴とするリモートアクセス方法。

【請求項２９】　前記端末離脱の検出において、
接続中の各端末がパケットを送出する毎に、自動的にタイマ値が増加する監視タイマをその端末用にセットし、該タイマ値が所定のスレッシュホールド値を超えた時、当該端末が離脱したと判定することを特徴とする請求項２８記載のリモートアクセス方法。

【請求項３０】　前記端末離脱の検出において、
当該リモートネットワークに接続中の各端末に対して所定時間毎に監視メッセージを送信し、該当端末から応答メッセージが返送されない場合に当該端末が離脱したと判定することを特徴とする請求項２８記載のリモートアクセス方法。

【請求項３１】　前記監視メッセージはＯＳＩのレイヤ３アドレスを含み、前記応答メッセージはＯＳＩのレイヤ２アドレスを含むことを特徴とする請求項３０記載のリモートアクセス方法。

【請求項３２】　コンピュータに請求項２８～３１いずれかに記載の方法を実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】ＬＡＮの有する利便性の１つである端末の移動をインターネットもしくはイントラネットを利用した広域のＬＡＮ環境においても実現するには、当該端末のネットワーク内での接続位置を特定する必要がある。このためには端末の接続と離脱の検出が必要となる。本発明は、このうち端末離脱の検出を実現する技術に関する。

【０００２】

【従来の技術】複数のサブネットワークが接続されたインターネットもしくはイントラネットにおいて、端末が移動しうる環境（仮想ＬＡＮシステム）を作ろうとすると、端末を収容するルータ等に端末の接続位置を管理する端末管理テーブルを設けてこのテーブルを端末の移動に合わせて自動更新する機能が必要である。このような機能を有する装置をクライアントと呼ぶ。

【０００３】上記のようなクライアントを有する仮想ＬＡＮ制御システムの一形態例を図１に示す。図１中、１０、２０、３０はインターネット上で仮想ＬＡＮを構築するサブネットワークをそれぞれ備えたオフィス、４０はインターネットである。なお、本発明はイントラネット等の同様のグローバルなパケット網に適用可能である。オフィス１０は着目している端末１０１、１０２が通常、接続されるサブネットワーク（以下、ホームネットワークと称し、”ＨＮＷ”と略称する）２００を備えており、以後、ホームオフィスと呼ぶものとする。ＨＮＷ２００には仮想ＬＡＮを構成するためのリモートアクセスサーバ（以下、”ＲＡＳ”と略称する）３０１が接続されており、また、ルータ４００を介してインターネット４０に接続されている。

【０００４】また、オフィス２０及び３０は前記端末１０１、１０２が移動した時に接続されるサブネットワーク（以下、リモートネットワークと称し、”ＲＮＷ”と略称する）５０１、５０２をそれぞれ備えており、以後、リモートオフィス２０及び３０と呼ぶものとする。ＲＮＷ５０１及び５０２には仮想ＬＡＮを構成するためのリモートアクセスクライアント（以下、”ＲＡＣ”と略称する）６０１及び６０２がそれぞれ接続されており、また、ルータ４００を介してインターネット４０に接続されている。また、インターネット４０にはルータ４００を介して仮想ＬＡＮを管理するための仮想ＬＡＮ管理サーバ（以下、”ＩＭＳ”と略称する）７００が接続されている。

【０００５】ここで、パケットの（アドレス）構成例を

図９に示す。図において、１００１がデータ、１００２がレイヤ２アドレス、１００３がレイヤ３アドレスを示す。それぞれのアドレスは発信と受信の２つのアドレスから構成される。詳しくはＯＳＩのレイヤ２はフレーム、レイヤ３はパケットと呼ばれるが、ここでは転送単位という意味でいずれについてもパケットと呼ぶ。パケット網においては、リンクレベルとネットワークレベルでそれぞれ異なるアドレスが付与される。レイヤ２アドレス１００２はＭＡＣアドレスとして知られており、端末製造時にベンダにより付与され、すべての端末を一意に識別できる情報である。一方、レイヤ３アドレス１００３はＩＰアドレスとして知られており、ネットワークレベルでの個々の端末を識別するために付与され、接続位置に対して固定的に付与され、パケットのルーチングに利用される。

【０００６】パケット網における端末間でのパケット転送例を図１０に示す。１１１から１１４までが端末、４０１と４０２がルータ、８００が通信経路である。この例では、端末１１１には、レイヤ２アドレス＃１、レイヤ３アドレス＃１が付与されている。図１０中の矢印は、端末１１２から端末１１３にパケットが転送される状態を示す。端末１１２がパケットを送信すると、コリジョン（衝突）ドメイン内の全端末である端末１１１と端末１１２、そしてルータ４０１に対してパケットがブロードキャストされる。各々の受け取り先では、パケットの着レイヤ２アドレスと自身のレイヤ２アドレスとの照合が行われる。一致すればパケットを取り込み、不一致の場合にはパケットを廃棄する。ここでは、ルータ４０１がパケットを受信することになる。

【０００７】ルータ４０１には、パケットの着レイヤ３アドレスと経路情報の対応表すなわちルーチングデータがあらかじめ保持されており、これに基づいてパケットの経路制御を実施する。この例では、通信先の端末１１３は経路８００に接続されているため、パケットを経路８００にルーチングする。このようにして最終的にはパケットは端末１１３に転送される。

【０００８】図１１は、パケット網に関して知られているアドレス解決法を説明するための図である。図において、４０１はルータ、１１１と１１２はルータ４０１の接続配下にある端末、９００はルータ４０１が保持するＡＲＰ（Address ResolutionProtocol）キャッシュである。このＡＲＰキャッシュは、通信先のレイヤ２アドレスとレイヤ３アドレスの対応を管理するためのメモリである。通信先のレイヤ３アドレスは分かるがレイヤ２アドレスが不明の場合、ＡＲＰキャッシュを利用してレイヤ２アドレスを取得する方法がＡＲＰとして知られている。

【０００９】ルータ４０１は、端末１１１のレイヤ２アドレスを取得しようとする場合、端末１１１のレイヤ３アドレスを設定したＡＲＰ要求パケットを接続配下の全端末に対してブロードキャストする。このＡＲＰ要求パケットを受信した該当する端末（１１１）は、自身のレイヤ２アドレスを含むＡＲＰ応答パケットを返送する。ルータ４０１は、このＡＲＰ応答パケットからレイヤ３アドレスを取り出してＡＲＰキャッシュ９００に保持し、以後の通信に用いる。なお、このＡＲＰキャッシュ９００の内容は、一定時間保持された後消去される。

【００１０】次に、図２は仮想ＬＡＮの初期情報管理テーブル５０を示すもので、本テーブルはＩＭＳ７００に初期設定され、以降、本テーブルを参照して仮想ＬＡＮの構成を行う。本テーブルは全仮想ＬＡＮ構成端末のＭＡＣアドレスとＨＮＷ２００のＲＡＳ３０１のＩＰアドレスとの対応テーブルである。

【００１１】図３は位置情報管理テーブル６０を示すもので、本テーブルはＩＭＳ７００及びＲＡＳ３０１に設定され、端末のＭＡＣアドレスと、端末が現在接続しているネットワークの位置情報であるＲＡＳあるいはＲＡＣのインターネットアドレス（ＩＰアドレス）との対応関係を管理する。このテーブルにより、ＩＭＳ７００及びＲＡＳ３０１は端末の位置をリアルタイムに管理することができる。

【００１２】図４はホームアドレス管理テーブル７０を示すもので、本テーブルはＲＡＣ６０１、ＲＡＣ６０２に設定され、リモートネットワークに接続中の端末のＭＡＣアドレスと、該端末のホームアドレスであるＲＡＳ３０１のＩＰアドレスとの対応関係を管理する。このテーブルにより、ＲＡＣ６０１、ＲＡＣ６０２は端末から送出されたパケットをＨＮＷ２００に転送することができる。

【００１３】図５は図１のシステムにおける自動認証シーケンスを示すものである。以下、図１の構成を例にとり、本システムにおける自動認証及び位置管理（移動時）の原理をこのシーケンスに従って説明する。まず、端末１０１がＨＮＷ２００からＲＮＷ５０１に移動する場合について説明する。

【００１４】ＨＮＷ２００の端末１０１がＲＮＷ５０１に移動した後、端末１０２宛に最初のパケット（ＭＡＣフレーム）を送出する場合（ステップＳ１、以下”ステップ”は省略）、ＲＮＷ５０１上に接続されたＲＡＣ６０１は前記パケットを獲得し、このパケット（ＭＡＣフレーム）における送信元端末１０１のＭＡＣアドレスを抽出し、該ＭＡＣアドレスが認証済みかどうかホームアドレス管理テーブル７０によりチェックする（Ｓ２）。

【００１５】ここではホームアドレス管理テーブル７０にエントリがないため（未認証）、ＩＭＳ７００にＴＥ１０１のＭＡＣアドレスとＲＡＣ６０１のＩＰアドレスを送出して該端末１０１の認証要求を出す（Ｓ３）。ＩＭＳ７００はＲＡＣ６０１からの認証要求に対して、送られてきた端末１０１のＭＡＣアドレスをもとに、仮想ＬＡＮシステム構築時に作成した上述した初期情報管理

テーブル５０により、認証及びホームアドレス解決を行う。

【００１６】即ち、端末１０１のMACアドレスが初期情報管理テーブル５０に存在すれば（Ｓ４）、ＲＡＣ６０１に対して認証ＯＫ及びＨＮＷ２００のＲＡＳ３０１のＩＰアドレスを返す（Ｓ５）。そして、ＩＭＳ７００は移動した端末１０１の位置情報管理テーブル６０を更新するとともに（Ｓ６）、移動した端末１０１のＨＮＷ２００のＲＡＳ３０１に対して、端末１０１のインターネット上の位置情報に相当するＲＡＣ６０１のＩＰアドレスを位置情報通知として送る（Ｓ７）。

【００１７】ＲＡＳ３０１は、自分の管理する端末の位置情報を位置情報管理テーブル６０上で更新する（Ｓ８）。ＲＡＣ６０１はＩＭＳ７００からの認証応答により、ホームアドレス管理テーブル７０を作成し、端末１０１のホームアドレスに相当するＲＡＳ３０１のＩＰアドレスを登録する（Ｓ９）。これにより認証及びアドレス解決が終了する。一方、端末１０１のMACアドレスが初期情報管理テーブル５０に存在しなければ、認証ＮＧをＲＡＣ６０１に返す（Ｓ１０）。ＲＡＣ６０１はＩＭＳ７００からの認証ＮＧにより、端末１０１から送出されるパケットを廃棄する（Ｓ１１）。

【００１８】図６は、前述した自動認証が終了した後、ホームネットワークに自動接続する場合のシーケンス例（端末１０１から端末１０２へのデータ送信）である。以下、本システムにおける自動接続及びマルチプロトコル対応の接続の原理をこのシーケンスに従って説明する。端末１０１が移動した先のリモートネットワークのＲＡＣ６０１は、端末１０１から（端末１０２宛の）パケット（MACフレーム）が送られてくると（Ｓ２１）、該端末が認証済みかどうかをホームアドレス管理テーブル７０によりチェックし、認証済みであることを確認する（Ｓ２２）。

【００１９】次に、ホームアドレス管理テーブル７０をもとに、端末のホームネットワークのＲＡＳ３０１に対して、端末１０１から送出されたパケットに対し、着ＩＰアドレス（ＤＡ）をＲＡＳ３０１、発ＩＰアドレス（ＳＡ）をＲＡＣ６０１としたＩＰヘッダ情報を付加してカプセル化し（Ｓ２４）、ＲＡＣ６０１よりＲＡＳ３０１に送信する（Ｓ２４）。

【００２０】ＲＡＳ３０１では、送られてきた、ＩＰヘッダ情報が含まれたパケットをデカプセル化し（Ｓ２５）、ＨＮＷ２００上に送出する。これにより、移動した端末１０１はあたかもＨＮＷ２００内でパケットを送ったように、ＲＮＷ５０１からＨＮＷ２００に接続されたＴＥ１０２へパケット（MACフレーム）を送出することが可能となる（Ｓ２６）。また、MACフレームをカプセル化することにより、ＯＳＩのレイヤ３以上のプロトコルに依存しない接続（即ち、マルチプロトコル）が可能となる。

【００２１】一方、ＨＮＷ２００上の端末１０２から、移動した端末１０１に対して送信する場合を図７に示す。この場合、端末１０２から送出されたパケット（MACフレーム）をＲＡＳ３０１がモニタする（Ｓ３１）。次に、位置情報管理テーブル６０により到着先MACアドレスの位置をチェックし（Ｓ３２）、移動した端末１０１のMACアドレスである場合はモニタしたパケットに対し、着ＩＰアドレス（ＤＡ）を移動先のＲＡＣ６０１、発ＩＰアドレス（ＳＡ）をＲＡＳ３０１としたＩＰヘッダ情報を付加してカプセル化し（Ｓ３３）、ＲＡＳ３０１よりＲＡＣ６０１に送信する（Ｓ３４）。ＲＡＣ６０１では、送られてきた、ＩＰヘッダ情報が含まれたパケットをデカプセル化し（Ｓ３５）、ＲＮＷ５０１上に送出することにより、移動した端末１０１にパケットが届けられる（Ｓ３６）。

【００２２】

【発明が解決しようとする課題】このような仮想ＬＡＮ制御システムにおいて、端末が任意の場所に移動できるようにするには、端末の接続位置を特定する必要があり、このためには端末の離脱の検出が必要となる。従来、これは端末を離脱するときに端末の利用者がこれから離脱する旨の指示を行い、この結果をクライアントに通知する方法で実現していた。この方法では端末に特別な機能を設けることが必要となり、市販の端末がそのまま利用できないという問題があった。本発明は、上記の問題を解決するために、端末に特別な機能を設けることなく端末の離脱検出を実現することを目的とする。

【００２３】

【課題を解決するための手段】上記課題を解決するために、本発明は、１つ以上の端末が通常時接続されるホームネットワークと、前記端末が移動時に接続される少なくとも１つのリモートネットワークとがグローバル・ネットワークを介して接続された仮想的なＬＡＮにおいて、

・前記ホームネットワークに接続され、前記グローバル・ネットワークのアドレスを有し、接続中の各端末の接続位置を示す管理テーブルを具備して、端末が前記リモートネットワークの１つに移動した時に該端末と前記ホームネットワークとのアクセスを、該端末が前記ホームネットワーク内でアクセスしているかのように制御するリモートアクセスサーバと、

・前記各リモートネットワークに接続され、前記グローバル・ネットワークのアドレスを有し、該リモートネットワークに接続中の各端末と前記ホームネットワークとの対応関係を示す管理テーブルを具備して、前記リモートネットワークと前記グローバル・ネットワークとの通信を制御するリモートアクセスクライアントと、

・前記グローバル・ネットワークに接続され、該グローバル・ネットワークのアドレスを有し、各端末と前記リモートアクセスサーバの対応関係及び、接続中の各端末

の接続位置を示す管理テーブルを具備して、端末の接続位置及びパケット送信を管理する仮想ＬＡＮ管理サーバとを有し、いずれかの端末が前記リモートネットワークの１つに接続され管理されている場合、該端末が送出するパケットのタイミングまたは該端末が更に他のリモートネットワークに移動した場合の接続情報に基づいて当該端末の当該リモートネットワークからの離脱を検出し、前記仮想ＬＡＮ管理サーバを介して端末離脱に伴うシステムの管理内容変更の制御を行う端末離脱検出システムを提供するものである。

【００２４】また、本発明は、上記のような仮想的なＬＡＮシステムにおいて、いずれかの端末が前記少なくとも１つのリモートネットワークの１つに接続され管理されている場合、該端末が送出するパケットのタイミングまたは該端末が更に他のリモートネットワークに移動した場合の接続情報に基づいて当該端末の当該リモートネットワークからの離脱を検出する端末離脱検出方法を提供する。

【００２５】前記端末離脱検出の好ましい方法として、以下のような方法がある。

（１）各リモートネットワークに接続中の各端末がパケットを送出する毎に、自動的にタイマ値が増加する監視タイマをその端末用にセットし、該タイマ値が所定のスレッシュホールド値を超えた時に当該端末が離脱したと判定する。

（２）端末が接続管理下の第１のリモートネットワークから第２のリモートネットワークに移動した場合、当該端末のパケットの送出を検出し、当該端末の管理情報から該端末がそれまで接続していたリモートネットワークが前記第１のリモートネットワークであることを認識し、該第１のリモートネットワークのリモートアクセスクライアントに該端末の離脱を通知する。

（３）前記リモートネットワークに接続中の各端末に対して所定時間毎に監視パケットを送信し、当該端末から応答パケットが返送されない場合に当該端末が離脱したと判定する。

【００２６】（１）の方法では、端末が離脱後に一定時間経過すれば、必ず端末離脱が検出できる。

（２）の方法では、端末が第１のリモートネットワークから第２のリモートネットワークに移動してパケットを送出すると直ちに離脱を検出できる。

（３）の方法は、通常のＡＲＰ手法による監視パケットの送出を利用して実現できる。また、これらの方法を組み合わせて行っても良い。

【００２７】また、本発明は、上記仮想ＬＡＮ制御システムにおける、対応する機能を有する仮想ＬＡＮ管理サーバ、即ち、前記グローバル・ネットワークに接続され、該グローバル・ネットワークのアドレスを有し、各端末と前記リモートネットワークのリモートアクセスサーバの対応関係及び、接続中の各端末の接続位置を示す管理テーブルを具備して、端末の接続状態及びパケット送信を管理する仮想ＬＡＮ管理サーバを提供するものであり、ここで、いずれかの端末が前記リモートネットワークの１つに接続され管理されている場合、該端末が更に他のリモートネットワークに移動した場合の接続情報に基づいて当該端末の当該リモートネットワークからの離脱を検出し、端末離脱に伴うシステムの管理内容変更の制御を行うことを特徴とする。

【００２８】更に、本発明は、上記仮想ＬＡＮ制御システムにおける、対応する機能を有するリモートアクセスクライアント、即ち、前記各リモートネットワークに接続され、前記グローバル・ネットワークのアドレスを有し、該リモートネットワークに接続中の各端末と前記ホームネットワークとの対応関係を示す管理テーブルを具備して、前記リモートネットワークと前記グローバル・ネットワークとの通信を制御するリモートアクセスクライアントを提供するものであり、ここで、いずれかの端末が前記リモートネットワークの１つに接続され管理されている場合、該端末が送出するパケットのタイミング情報に基づいて当該端末の当該リモートネットワークからの離脱を検出することを特徴とする。

【００２９】また、本発明は、これらサーバやクライアントに対応する方法及び、それら方法を実行させるためのプログラムを記録したコンピュータ読み取り可能な記憶媒体を提供するものである。

【００３０】

【発明の実施の形態】以下、図面を参照して、本発明の実施形態について説明する。以下の説明において、仮想ＬＡＮ制御システムの基本構成は、上述した図１の構成と同一である。

【００３１】図８は、本発明による端末離脱シーケンスの一例であり、ＲＮＷ５０１に移動した端末１０１が再びＨＮＷ２００に移動する際の例である。ＲＡＣ６０１では端末１０１がパケット（ＭＡＣフレーム）を送出する毎に（Ｓ４１）、時間の経過に合わせて自動的にタイマ値が増加する端末離脱監視タイマをリセットし（Ｓ４２）、このタイマ値があるスレッショルド値をこえた時（Ｓ４３）、ＲＮＷ５０１より離脱したとみなす（Ｓ４４）。このタイマの利用により、端末側のプロトコルに依存しないマルチプロトコル対応の離脱が可能となる。ＲＡＣ６０１ではタイムアウトを検出すると、ＩＭＳ７００に対し、端末が離脱したことを示す端末離脱要求パケットを送出する。該パケットの内容は、ＴＥ１０１のＭＡＣアドレスとＲＡＣ６０１のＩＰアドレスを有したものとなっている（Ｓ４５）。

【００３２】ＩＭＳ７００では該パケットを受信すると、位置情報管理テーブル６０の端末１０１に関する内容を、端末１０１が移動していたリモートネットワークのＲＡＣ６０１のＩＰアドレスから、端末１０１のデフォルト位置であるＨＮＷ２００のＲＡＳ３０１のＩＰア

ドレスに更新する（Ｓ４６）。また、ＲＡＣ６０１には端末離脱応答パケットを送出し（Ｓ４７）、ＲＡＳ３０１には端末１０１のＭＡＣアドレスとＲＡＣ６０１のＩＰアドレスを付けて端末離脱通知を送出する（Ｓ４８）。

【００３３】ＲＡＣ６０１では、端末離脱応答をＩＭＳ７００から受信することによって、端末のホームアドレス管理テーブル７０の該端末のエントリを削除することにより端末離脱処理を完了する（Ｓ４９）。ＲＡＳ３０１はＩＭＳ７００からの端末離脱通知を受信すると、端末１０１の現在の接続位置を登録するために位置情報管理テーブル６０を更新する（Ｓ５０）。

【００３４】この方法によれば、端末が離脱した後で一定時間経過すれば必ず端末離脱が検出できる。そして、端末の位置を管理する管理テーブルが移動に合わせて自動更新されるので、端末がネットワーク間を移動しても環境の再設定は不要である。しかしながら、端末が通信する頻度と通信時間の特性を考慮してどの端末にも当てはまるようにスレッショルド値を決めるため、端末離脱の検出に遅れが出る可能性がある。

【００３５】図１２に、本発明による端末離脱シーケンスの第２の例を示す。本実施例は、端末１０１がＲＮＷ５０１からＲＮＷ５０２に移動する場合の例である。端末１０１がＲＮＷ５０２に移動後にパケットを送信すると（ステップＳ６１）ＲＡＣ６０２がこれを検出し、端末１０１が接続したことを通知する端末接続通知パケットをＩＭＳ７００に送出する（ステップＳ６２）。ＩＭＳ７００では、このパケットを受信すると、位置情報管理テーブル６０を検索して端末１０１が移動したこと、そして移動前まで接続していたＲＮＷが５０１であることを認識する（ステップＳ６３）。そして、端末１０１が移動したことを示す端末離脱通知パケットをＲＡＣ６０１に通知する（ステップＳ６４）。

【００３６】ＲＡＣ６０１はこのパケットを受信すると端末１０１が離脱したことを知り、自身のホームアドレス管理テーブル７０の端末１０１に関する情報を削除し、離脱処理を行う（ステップＳ６５）。同時に、ＩＭＳ７００は、端末１０１が移動したことを示す端末接続位置通知パケットをＲＡＳ３０１に通知する（ステップＳ６６）。この方法では、端末が移動（離脱）後に通信を行おうとするまでは離脱が検出できないが、通信を開始すると離脱が直ちに検出できるという長所を有する。上記第１と第２の例に示すいずれかの方法のみで離脱を検出しても良いし、両方の方法を併用して検出しても良い。２つの方法を併用することにより、端末離脱がより正確に検出できる。

【００３７】２つの方法を併用したシーケンス例を図１３に示す。本例もまた、ＲＮＷ５０１にそれまで接続され通信していた端末１０１がＲＮＷ５０２に移動し通信を開始した場合である。即ち、ＲＮＷ５０１にそれまで接続されていた端末１０１がＲＮＷ５０２に移動後に通信を行おうとしてパケットを送信すると（ステップＳ７１）、ＲＡＣ６０２がこれを検出し、自身のホームアドレス管理テーブル７０を検索するが、ここでは端末１０１についてのレコードがないため、ＲＡＣ６０２は端末１０１が新たに接続されたことを知る（ステップＳ７２）。

【００３８】ＲＡＣ６０２は、端末１０１のＭＡＣアドレスと自身の識別情報（ＩＰアドレス）を含む端末接続通知パケットをＩＭＳ７００に送信する（ステップＳ７３）。ＩＭＳ７００はこのパケットを受信すると、パケットに含まれた情報に基づいて自身の初期情報管理テーブル５０を検索する（ステップＳ７４）。端末１０１はこのテーブルに関しては登録済みであるため、ＩＭＳ７００は、端末１０１が認証されたことをＲＡＣ６０２に通知し（ステップＳ７５）、ＲＡＣ６０２は、自身の管理テーブル７０に端末１０１のレコードを追加する（ステップＳ７６）。また、同時に、ＩＭＳ７００はＲＡＳ３０１に、端末１０１の新たな接続位置を示す端末接続位置通知パケットを送信する（ステップＳ７７）。

【００３９】ＲＡＳ３０１はこのパケットを受信すると、自身の位置情報管理テーブル６０の端末１０１の接続位置に関するデータを更新する（ステップＳ７８）。一方、ＩＭＳ７００側では、管理テーブル６０を検索すると端末１０１はそれまでＲＡＣ６０１に接続されていたことが分かるので、ＲＡＣ６０１に端末離脱通知パケットを送信する（ステップＳ７９）。ＲＡＣ６０１はこのパケットを受信すると自身の管理テーブル７０から端末１０１に関するレコードを削除し、端末離脱処理を行う（ステップＳ８０）。

【００４０】一方、ＲＡＣ６０１が保持する端末１０１に関する端末離脱監視タイマは、端末１０１から最後のパケットを受信した時点からタイマ値が時間の経過に合わせて増加する。そのため、一定時間経過するとこのタイマがタイムアウトし、端末離脱が検出される（ステップＳ８１）。この結果、ＲＡＣ６０１は自身の管理テーブル７０から端末１０１に関するレコードを削除し端末離脱処理を行う（ステップＳ８０）。

【００４１】従って、ＲＡＣ６０１は、端末離脱通知パケットの受信もしくは端末離脱監視タイマのタイムアウトのいずれか早い方の情報で端末１０１の離脱が検出できる。即ち、端末が離脱後通信を再開しなくても一定時間経過すると端末離脱監視タイマを利用する第１の方法で、一方、端末が離脱後早い時期に新たなＲＮＷで通信を再開した場合には第２の方法で端末離脱を検出できる。このように２つの方法を併用すると、より正確に端末離脱が検出でき、また、もちろんこの場合も端末に特別な機能を設ける必要はない。

【００４２】図１４に、本発明による端末離脱シーケンスの第３の例を示す。本例は、端末の離脱の検出を、上

述したＡＲＰの手法を応用して実現しようというものである。本例は、端末１０１がＨＮＷ２００からＲＮＷ５０１に移動して通信を行おうとする場合の例である。端末１０１が移動後に新たに第１のパケットを発信すると（ステップＳ９１）、パケット送出を検出したＲＡＣ６０１は自身の管理テーブル７０を検索する。ここで、端末１０１に関する登録情報は見つからないため、ＲＡＣ６０１はＩＭＳ７００に端末認証要求パケットを送信する（ステップＳ９２）。このパケットは端末１０１のＭＡＣ（レイヤ２）アドレスと要求元ＲＡＣの識別情報（ＩＰアドレス）を含む。

【００４３】ＩＭＳ７００では、このパケットに含まれたＭＡＣアドレスから初期情報管理テーブル５０を検索して端末１０１が登録済み端末であることを認証する（ステップＳ９３）。また、位置情報管理テーブル６０を検索して端末１０１の接続位置がＨＮＷ２００からＲＮＷ５０１に移動したことを知り、端末１０１の新たな接続先を管理するために、テーブル６０の該当レコードを更新する（ステップＳ９４）。そして、認証結果パケットをＲＡＣ６０１に返送する（ステップＳ９５）。

【００４４】このパケットにより端末１０１は登録済みであることが認証されたため、ＲＡＣ６０１では、当該パケットの内容に基づいて自身の管理テーブル７０に端末１０１のＭＡＣアドレス情報を追加する（ステップＳ９６）。次に、端末１０１が第２以降のパケットを転送すると（ステップＳ９７）、ＲＡＣ６０１はこのテーブル７０の情報を用いてこれを認証し、パケットを中継する（ステップＳ９８）。

【００４５】ＲＡＣ６０１は、自身の管理テーブル７０に記録されている各端末に対して、所定の時間毎に、端末のＩＰ（レイヤ３）アドレスを設定し、そのＭＡＣ（レイヤ２）アドレスを問い合わせる監視パケットを送信する（ステップＳ９９）。即ち、端末１０１に対しても監視パケットが送信されるが、この監視パケットの着信ＩＰアドレスは端末１０１に設定されているので、端末１０１がＲＮＷ５０１から離脱すると（ステップＳ１００）、予期される応答パケットが返送されない。

【００４６】一定時間経てもＲＡＣ６０１に応答パケットが返送されない場合、ＲＡＣ６０１は端末１０１は離脱したものと判断する（ステップＳ１０１）。この場合、自身の管理テーブル７０の該当レコードを削除する（ステップＳ１０２）とともに、ＩＭＳ７００に端末離脱通知パケットを送信する（ステップＳ１０３）。ＩＭＳ７００は、端末離脱通知パケットを受信すると自身の位置情報管理テーブル６０内の端末１０１に関するレコードの現在の接続位置をデフォルト位置であるＨＮＷ２００のＲＡＳ３０１のＩＰアドレスに変更する（ステップＳ１０４）。更に、ＩＭＳ７００は、端末１０１のＨＮＷのＲＡＳ３０１に端末離脱通知パケットを送信する（ステップＳ１０５）。ＲＡＳ３０１もまた、自身の位

置情報管理テーブル６０の内容を、端末１０１の移動に合わせ更新する（ステップＳ１０６）。

【００４７】即ち、この例の場合、端末１０１の離脱後一定時間経ると、ＡＲＰ手法を利用した監視パケット（及び応答パケット）により離脱が検出できる。即ち、ＲＡＣ、ＲＡＳ、ＩＭＳ側に端末の移動を自動検出する機能を設けることにより、端末に特別な機能を設けなくても端末離脱が検出できる。

【００４８】

【発明の効果】即ち、本発明によれば、仮想ＬＡＮ制御システムにおいて端末が任意の場所に移動できるようにするために必要な端末離脱の検出が、端末に特別なシステムや手順を設定することなく実現できる。

【図面の簡単な説明】

【図１】　本発明に関する仮想ＬＡＮ制御システムの構成例である。

【図２】　初期情報管理テーブルの一例を示す図である。

【図３】　位置情報管理テーブルの一例を示す図である。

【図４】　ホームアドレス管理テーブルの一例を示す図である。

【図５】　本仮想ＬＡＮ制御システムにおける自動認証シーケンスを示す図である。

【図６】　本システムにおける自動接続シーケンス例を示す図である。

【図７】　本システムにおける自動接続シーケンス例示す図である。

【図８】　本発明による自動離脱シーケンス例を示す図である。

【図９】　パケットのアドレス構成例を示す図である。

【図１０】　パケット転送例を示す図である。

【図１１】　アドレス解決法の例を示す図である。

【図１２】　本発明による自動離脱シーケンス例を示す図である。

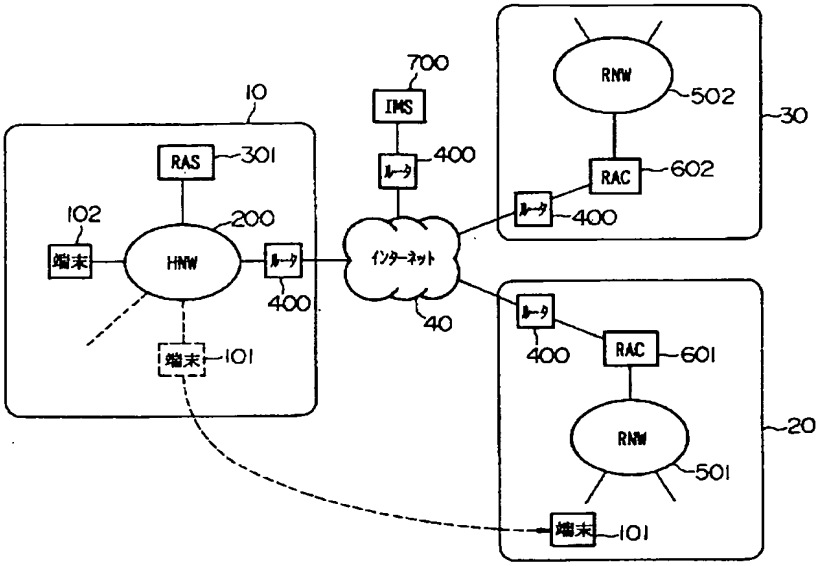
【図１３】　本発明による自動離脱シーケンス例を示す図である。

【図１４】　本発明による自動離脱シーケンス例を示す図である。

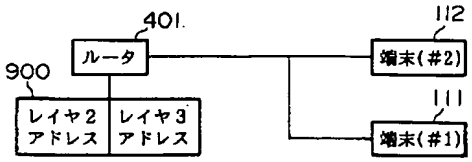
【符号の説明】

１０…ホームオフィス、２０，３０…リモートオフィス、４０…インターネット、５０…初期情報管理テーブル、６０…位置情報管理テーブル、７０…ホームアドレス管理テーブル、２００…ＨＮＷ（ホームネットワーク）、５０１，５０２…ＲＮＷ（リモートネットワーク）、３０１…ＲＡＳ（リモートアクセスサーバ）、６０１，６０２…ＲＡＣ（リモートアクセスクライアント）、１０１，１０２…端末、７００…ＩＭＳ（仮想ＬＡＮ管理サーバ）、４００…ルータ。

【図１】



【図１１】



【図２】

端末のMACアドレス	端末のホームネットワークアドレス（RASのIPアドレス）
端末１０１のMACアドレス	RAS３０１のIPアドレス
端末１０２のMACアドレス	RAS３０１のIPアドレス
⋮	⋮

50

【図３】

端末のMACアドレス	端末の位置情報（RAS or RACのIPアドレス）
端末１０１のMACアドレス	RAS３０１のIPアドレス
端末１０２のMACアドレス	RAS３０１のIPアドレス
⋮	⋮

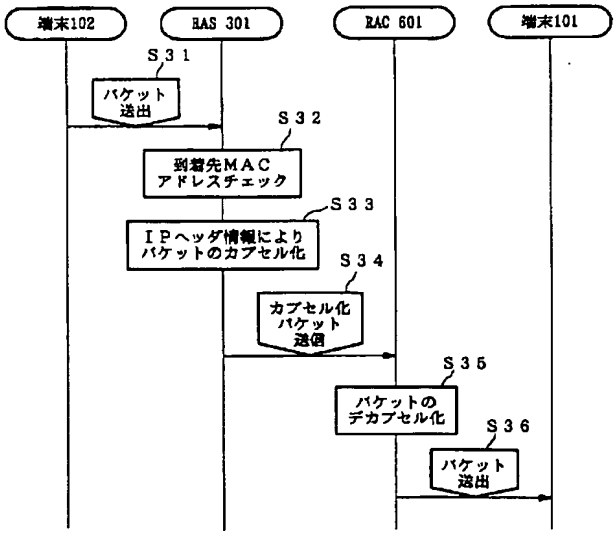
60

【図４】

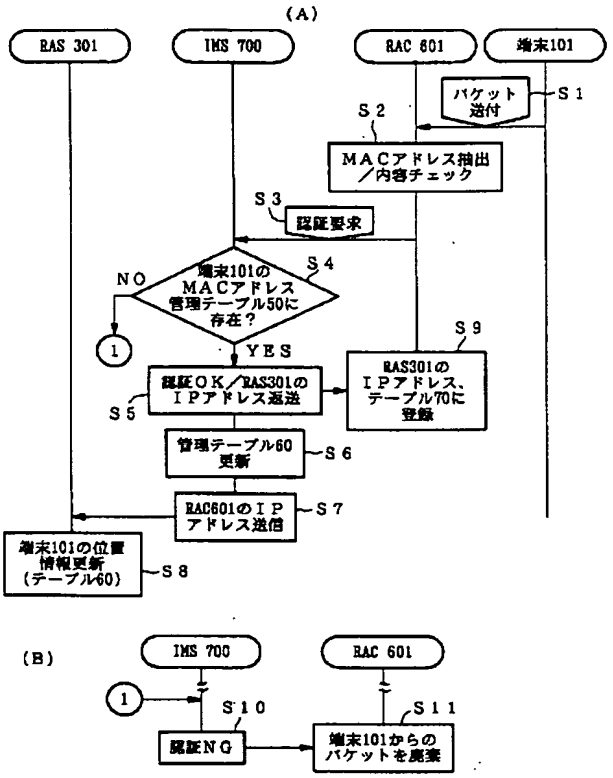
移動端末のMACアドレス	移動端末のホームアドレス（RASのIPアドレス）
端末１０１のMACアドレス	RAS３０１のIPアドレス
⋮	⋮

70

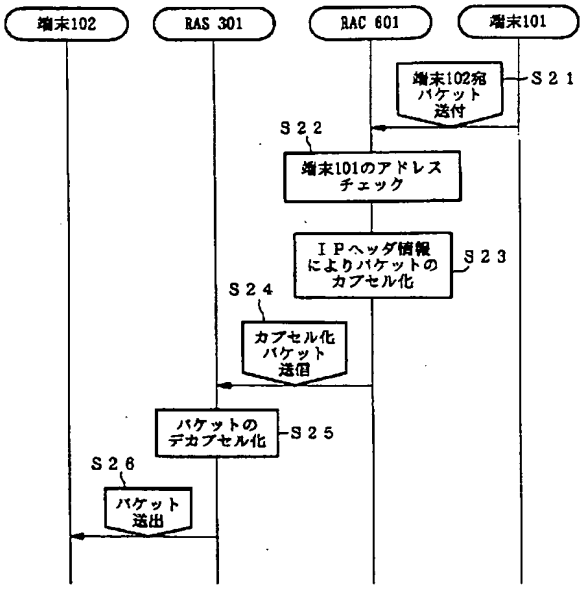
【図７】



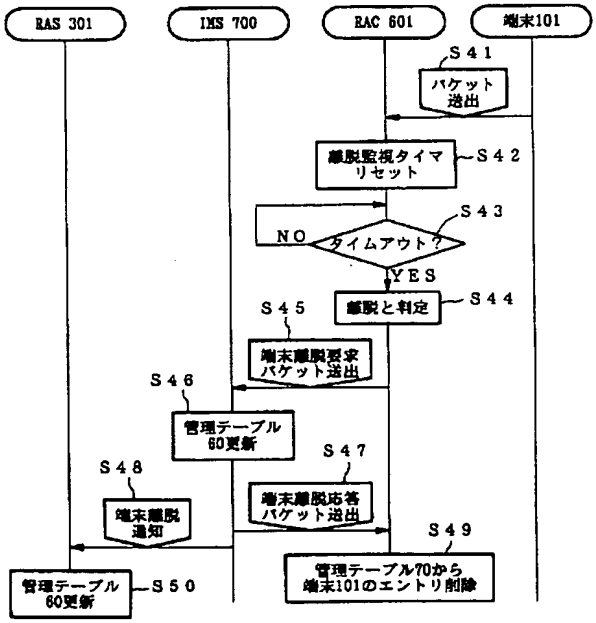
【図５】



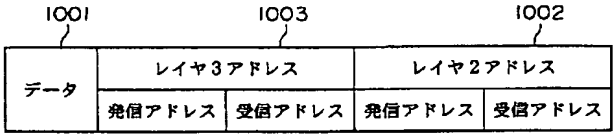
【図６】



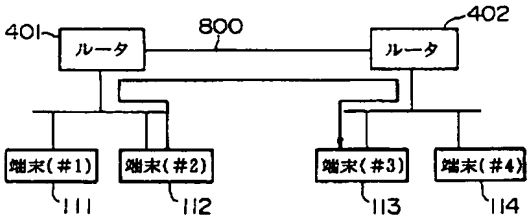
【図８】



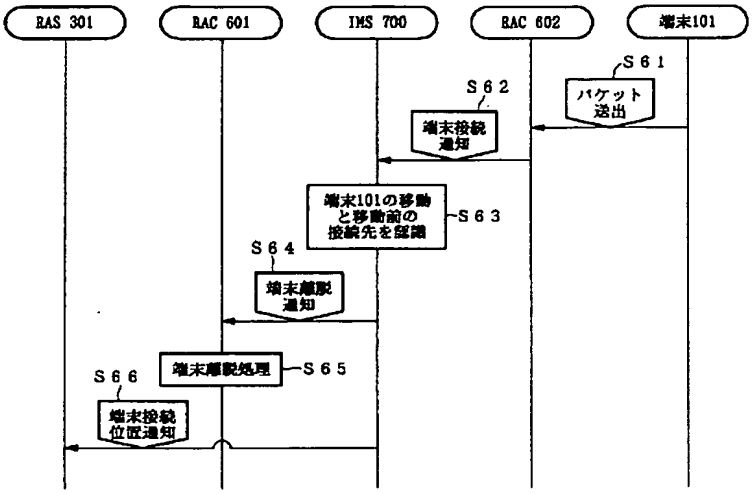
【図９】



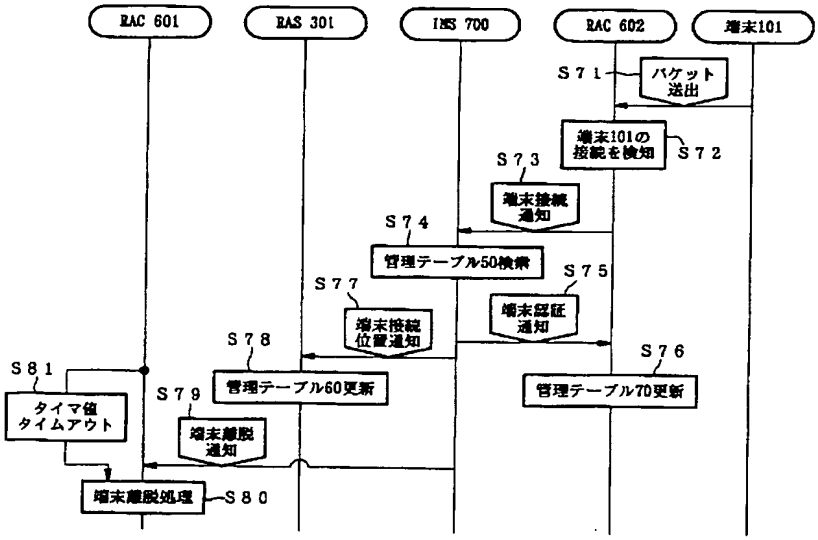
【図１０】



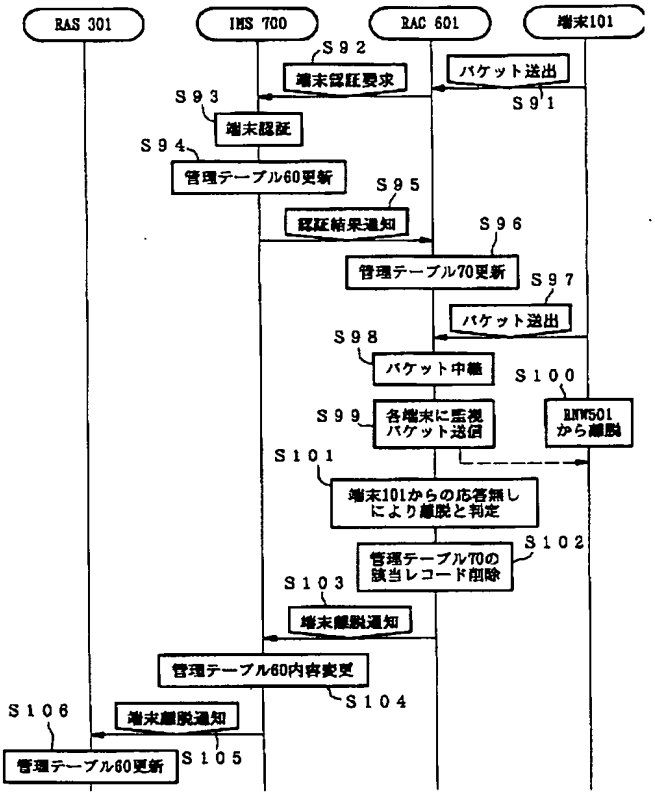
【図１２】


RAS 301
RAC 601
IMS 700
RAC 602
端末101
S61
パケット送出
S62
端末接続通知
端末101の移動と移動前の接続先を認識
S63
S64
端末離脱通知
端末離脱処理
S65
S66
端末接続位置通知

【図１３】


RAC 601
RAS 301
IMS 700
RAC 602
端末101
S71
パケット送出
端末101の接続を検知
S72
S73
端末接続通知
S74
管理テーブル50検索
S75
端末認証通知
S77
端末接続位置通知
S78
管理テーブル60更新
S76
管理テーブル70更新
S81
タイマ値タイムアウト
S79
端末離脱通知
端末離脱処理
S80

【図１４】



フロントページの続き

(72)発明者　増井　貴
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　永井　浩一
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内